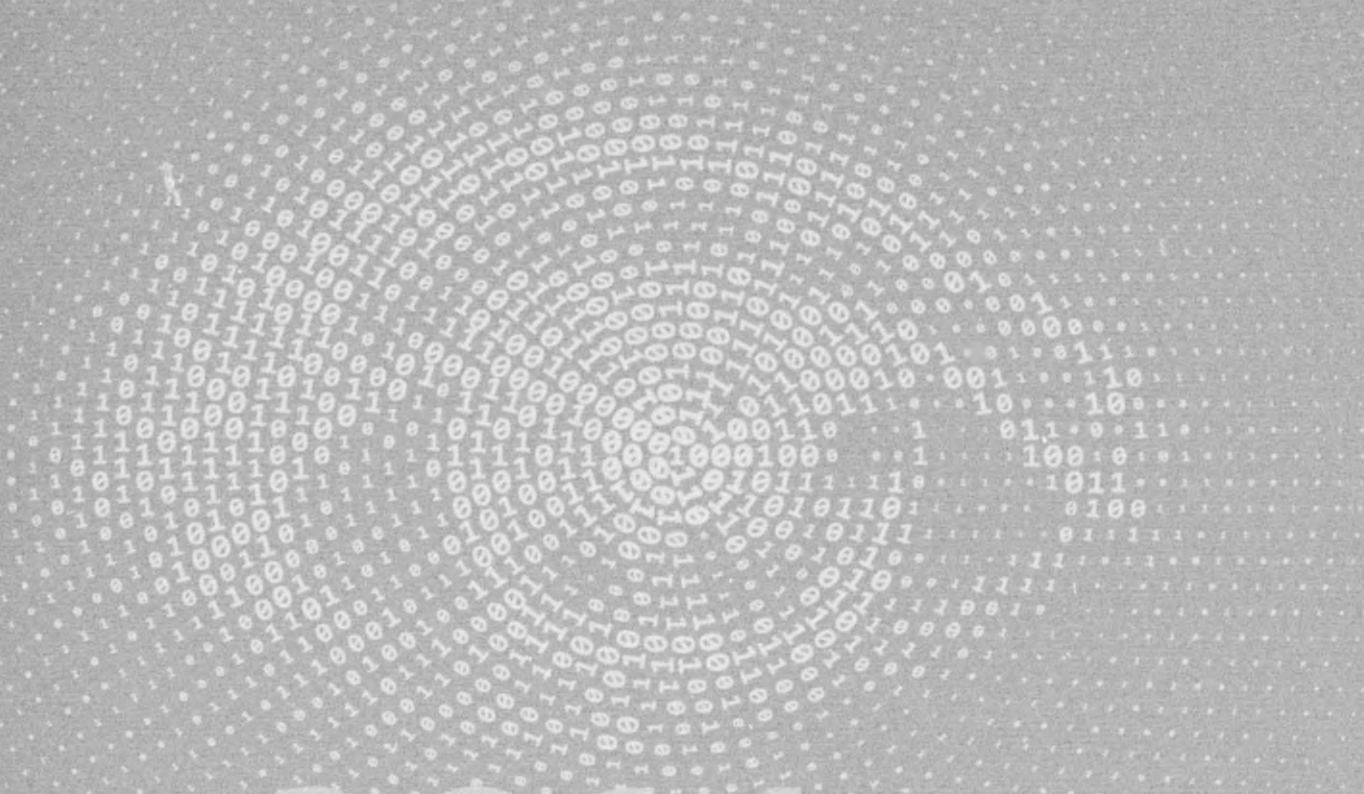
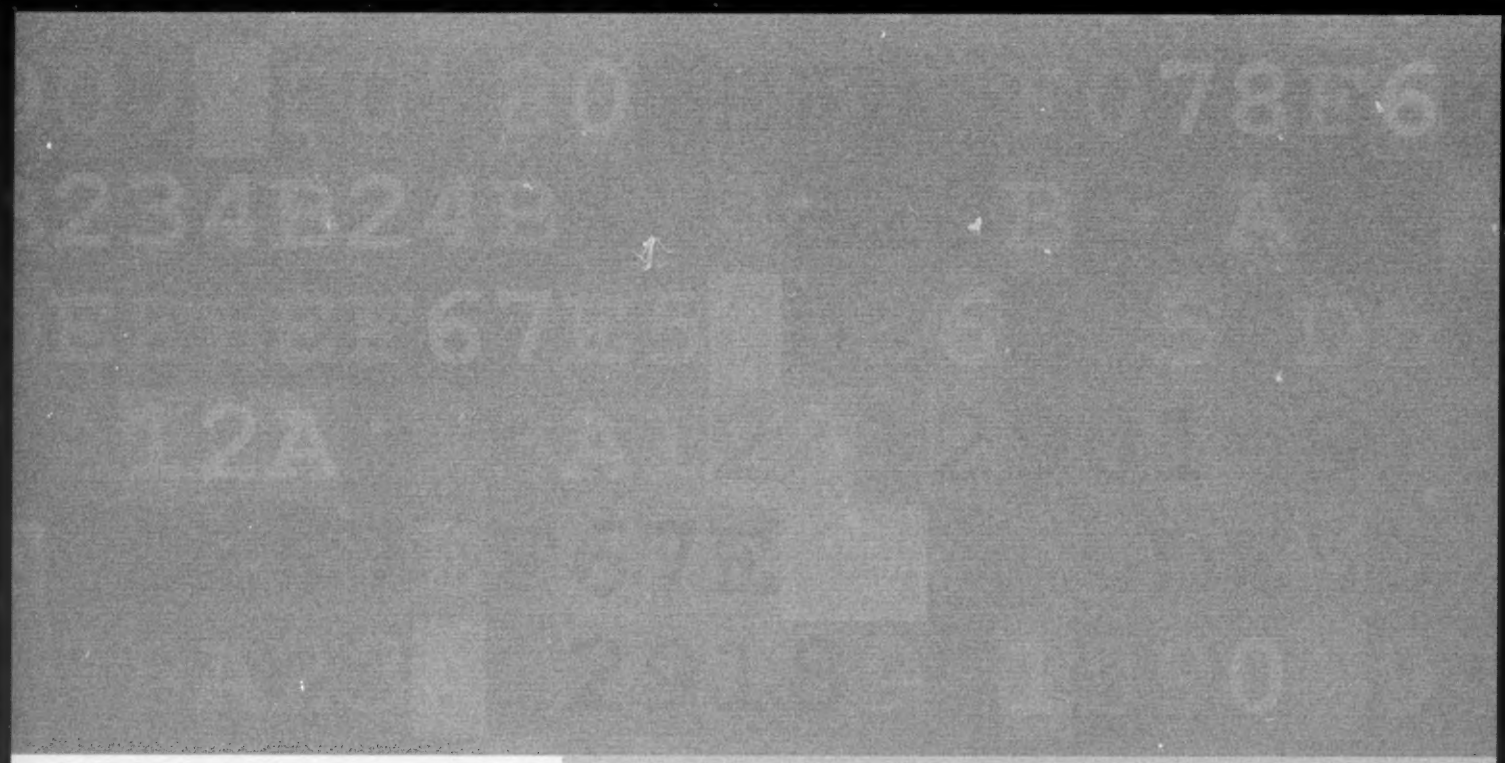
Office of the Information and Privacy Commissioner for British Columbia



ANNUAL REPORT 2014 2015

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.



What We Do

Established in 1993, the Office of the Information and Privacy Commissioner ("OIPC") provides independent oversight and enforcement of B.C.'s access and privacy laws, including:

- The ***Freedom of Information and Protection of Privacy Act*** ("FIPPA"), which applies to over 2,900 "public bodies," including ministries, local governments, schools, crown corporations, hospitals, municipal police forces and more; and
- The ***Personal Information Protection Act*** ("PIPA"), which applies to over 380,000 private sector "organizations," including businesses, charities, associations, trade unions and trusts.

Elizabeth Denham is B.C.'s Information and Privacy Commissioner.

Our Vision

- A community where privacy is valued, respected and upheld in the public and private sectors;
- A community where access to information rights are understood and robustly exercised; and
- A community where public agencies are open and accessible to the citizenry they serve.

Strategic Goals

1. Uphold privacy rights and monitor protection of personal information and data.
2. Ensure public bodies and private sector organizations understand their responsibilities under the law.
3. Promote and advocate for an open, accountable and transparent public sector.
4. Help individuals understand the value of information rights and to make informed choices about the exercise of those rights.
5. Enhance the quality and capacity of the OIPC's people, systems, processes and culture.

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

June 2015

The Honourable Linda Reid
Speaker of the Legislative Assembly
of British Columbia
Room 207, Parliament Buildings
Victoria, BC V8V 1X4

Honourable Speaker:

In accordance with s. 51 of the *Freedom of Information and Protection of Privacy Act* and s. 44 of the *Personal Information Protection Act*, I have the honour to present the Office's Annual Report to the Legislative Assembly.

This report covers the period from April 1, 2014 to March 31, 2015.

Yours sincerely,

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

Table of Contents

Commissioner's Message	4
Our Work	6
Highlights 2014-15	8
Special Reports	10
Investigation Reports	12
Compliance Summary	13
Privacy Watch	14
Global Guardians	16
Protecting Privacy in Hiring	18
Mandate for Change	20
In Data We Trust	22
Year in Numbers	24
Financial Reporting	33
Resources	35

COMMISSIONER'S MESSAGE

> "Technology will continue to accelerate in ways we cannot yet imagine. As data use by business and government intensifies, trust, transparency and individual control are vital."
>
> — Elizabeth Denham,
> *Information and Privacy Commissioner for British Columbia*

When I was appointed Information and Privacy Commissioner for British Columbia in 2010, emerging technologies were opening up new and promising in-roads for access to information. They were also presenting challenges to personal privacy. With this backdrop, my primary objective was to create a more proactive and effective regulatory role for this Office.

A proactive approach to information rights is essential in our digital society. As massive privacy breaches continue to make headlines and the capacity for businesses and government to collect, combine and analyze data grows, citizens are increasingly aware of the potential for their data to be misused or misplaced, whether by accident or through a malicious intent. Their legitimate concerns about misuse of their personal information had a direct correlation to our Office's increased workload this fiscal year. Calls and emails from the public spiked to 5,200 individual requests for information, an increase of almost 30% from 2013-14. These concerns continue to increase, along with challenges to ensure protection of our fundamental rights to access government information and personal privacy. As an oversight agency, we cannot chase every rabbit we see; we must be strategic about the investigations we pursue in order to maximize the educational and compliance impact of our work.

My Office's comprehensive report into the misuse of police information in employment background checks exemplifies this proactive approach. At the time of our investigation, police agencies in this province routinely disclosed sensitive, non-conviction information as well as information about police apprehensions of individuals under the *Mental Health Act* as part of employee and volunteer screening. We knew this practice was creating very real privacy harms for individuals — many innocent British Columbians with no criminal records had their professional and personal lives affected by information disclosed from police databases. We shared their words in our public report issued in April 2014 to illustrate the privacy implications of these disclosures. My recommendation to end the disclosure of mental health information in all police information checks and to prohibit or limit the disclosure of non-conviction information was adopted by government in a new policy directive, which has been endorsed by all B.C. police agencies, including the RCMP.

Similarly, our investigation into the District of Saanich's use of employee monitoring software was an opportunity to both review the District's compliance with privacy laws as well as to make it very clear that employees do not check their privacy rights at the office door. The report made five recommendations to address the compliance issues arising in Saanich, including the need for a Privacy Officer and a comprehensive privacy management program. All of the recommendations have been adopted by the District and Council.

In 2014-15, we also encouraged others to be more proactive. In January, I released a Special Report, the first in our Office's new Audit and Compliance program, examining the B.C. Government's privacy breach management. We found that suspected breaches across government were investigated promptly by the Office of the Chief Information Officer, but there was no systematic follow up or analysis of the causes of breaches across ministries, and no safeguards in place to make sure privacy and security recommendations were being followed. In the report, I recommended that government address the root causes of breaches and engage in learning and future prevention. I also recommended that all suspected breaches be reported to my Office whenever there is potential for harm or a large number of individuals may be affected. In *A Step Backwards*, my Special Report on timeliness, I urged government to be proactive in the disclosure of high-demand categories of information, such as calendars, by individuals requesting records under the freedom-of-information process. And in *A Failure to Archive*, I called upon the Ministry of Technology, Innovation and Citizens' Services and the Royal BC Museum to take charge of the tens of thousands of boxes containing valuable government records that had been accumulating in warehouses for more than 10 years, and create a modern records management system for the people of this province. An agreement is now in place between the Ministry and the Museum to do just that.

And since proactivity begins at home, our Office began a close examination of our own operations to address the growing workloads that have resulted from the increased demand for our services. The objective is to find internal efficiencies that will enable us to resolve and close investigation files faster, reducing wait times for the public while assisting public and private sector organizations more efficiently. This was the first time in more than 20 years that we have taken such a deep look at our internal processes, and I look forward to reporting the results of these efforts to you in 2015-16.

Technology will continue to accelerate in ways we cannot yet imagine. As data use by business and government intensifies, trust, transparency and individual control are vital. Citizens and consumers need to trust that their personal data is protected, and governments and organizations need to build privacy protection into their products and protocols, to build the loyalty and confidence of those they serve. Adopting a modern approach to regulation — moving from a complaints-based organization to one that advises and reviews schemes and systems before agencies press "go," reaching out to public bodies and organizations in speeches and conferences, publishing guidelines and initiating systemic investigations and audits when it is in the public interest — encourages an environment of trust.

In closing, I would like to acknowledge the dedication and teamwork of my staff, the support of our External Advisory Board, as well as the stakeholders in the access and privacy community. Their ongoing interest, involvement and dedication contribute significantly to the work of this Office.

Elizabeth Denham
Information and Privacy Commissioner for British Columbia

OUR WORK

Commissioner

The Information and Privacy Commissioner, an independent Officer of the Legislature, oversees the privacy practices of public bodies and private organizations. She has the legal authority to investigate programs, policies or information systems in order to assess compliance with B.C.'s access and privacy laws. The Commissioner also reviews appeals of access to information responses, comments on the implications of new programs, policies and technologies on access and privacy rights and engages in public education and outreach activities.

In 2014-15, the Commissioner gave 82 media interviews, an increase of 30% over last year.

Intake Services

The Intake Service Officer responds to access and privacy questions, complaints and inquiries received through the Info Line and email information box. Intake Officers help individuals seeking a review of an access to information request or filing a complaint. This includes screening, determining issues and providing assistance to individuals to complete related forms and letters and initiate appropriate action. Intake officers are also first responders to breach notifications and can assist in the early resolution of complaints.

In 2014-15, Intake Officers received 132 privacy breach notifications, an increase of nearly 16% over the previous year. There were 5,200 requests for information, an increase of almost 30% over 2013-14.

Investigation & Mediation

Complaints and appeals of access to information requests are assigned to OIPC Investigators, who review the facts and any records at issue and work with the complainant and the public body to reach a resolution.

In 2014-15, 99% of all complaints were resolved without a hearing or inquiry; no change over 2013-14.

Adjudication

When a complaint or review cannot be resolved between the parties, the Commissioner or her delegate will conduct a formal inquiry. Adjudicators assess the evidence and arguments of parties and issue final and binding decisions that have the force of a court of law. Orders can be appealed to the B.C. Supreme Court.

In 2014-15, the Office issued 66 orders, an increase of more than 74% over the previous year.

Policy & Technology

Policy Analysts conduct research and analyze current and emerging access and privacy issues, conduct systemic investigations, review and comment on privacy impact assessments and consult with public bodies and private organizations. They also review and analyze proposed legislation with an eye to the implications for access and privacy rights of British Columbians.

In 2014-15, 170 policy or issue consultation files were opened by policy analysts, an increase of more than 100% over the previous year. Closed files: 150

Audit & Compliance

The Audit & Compliance team proactively assesses the extent to which public bodies and private sector organizations are protecting personal information and complying with access provisions under the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act*.

In 2014-15, the Commissioner published the first audit report, *An Examination of B.C. Government's Privacy Breach Management*. The OIPC examination team selected a sample of 327 government privacy breach investigation files from 2012 and 2013 for this review.

Communications

The Communications team helps publicize the Commissioner's work and engages in public education and outreach to inform and empower individuals to exercise their information and privacy rights. The Office's website, social media presence, media relations, corporate reporting and proactive disclosure programs are managed by the Communications team.

In 2014-15, OIPC Communications fielded 262 media requests, an increase of 46% over the previous year.

HIGHLIGHTS 2014-15

New Guidance for Police on Body-Worn Cameras

The OIPC collaborated with Privacy Commissioners across Canada to produce a guidance document for law enforcement agencies considering the use of body-worn cameras. The document offers practical advice and addresses the significant privacy issues related to these devices, which record not only video and audio of an individual but also that person's associations with others within recording range, including friends, family members, bystanders, victims and suspects.

READ: *Guidance for the Use of Body-Worn Cameras by Law Enforcement Authorities* (oipc.bc.ca).

OIPC Rules on Ministry's Reference Checking Practice

Following a complaint, an Adjudicator made an important ruling affecting a Ministry's reference checking practices. An individual applied for a job and provided the names of references. The Ministry chose to speak to other individuals, without advising the complainant or obtaining her consent to do so. The Adjudicator ruled that asking others about the individual was contrary to FIPPA and ordered the Ministry to stop collecting personal information and destroy any previously collected personal information.

DOWNLOAD: *Order F14-26* (oipc.bc.ca).

DOWNLOAD: *Checking References: Guideline for Public Bodies* (oipc.bc.ca).

Canada's Privacy Commissioners React to Bill C-51

Commissioner Elizabeth Denham joined other privacy commissioners across Canada to voice concern about the privacy implications of Bill C-51, federal legislation aimed at increasing powers for law enforcement and intelligence agencies.

READ: *Privacy Watch*, page 14.

Asia-Pacific Privacy Authorities (APPA) Forum Hosted in Vancouver

The OIPC welcomed 130 APPA colleagues and delegates to Vancouver in December 2014. The privacy regulators meet twice each year to form partnerships and collaborate on privacy enforcement.

READ: *Global Guardians*, page 16.

Commissioner Examines Government's Failure to Archive

The Commissioner published a Special Report about the state of British Columbia's archives. Tens of thousands of boxes of government records — a 10-year backlog — await transfer and preservation in the BC Archives. The Commissioner concluded that an "archiving stalemate" had developed because government was not allocating sufficient resources to archive new records and made recommendations to rectify the situation.

READ: *Special Reports Summary*, page 10.

DOWNLOAD: *A Failure to Archive: Recommendations to Modernize Government Records Management* (oipc.bc.ca).

Special Report on Privacy Protection in B.C.'s Health Sector

B.C. needs a new health information law to improve patient care and protect privacy, stressed the Commissioner in one of this Special Report's 21 recommendations.

READ: *Special Reports Summary*, page 10.

DOWNLOAD: *A Prescription for Legislative Reform: Improving Privacy Protection in B.C.'s Health Sector* (oipc.bc.ca).

Police Information Checks Examined

Calling it her most important Investigative Report to date, the Commissioner urged police forces to stop disclosing non-conviction information in background checks for employment purposes.

READ: *Protecting Privacy in Hiring*, page 18.

DOWNLOAD: *Use of Police Information Checks in British Columbia* (oipc.bc.ca).

Use of Employee Monitoring Software in Saanich

Following a high profile investigation, the Commissioner recommended that the District of Saanich disable key features of its employee monitoring software including keystroke logging, automated screen shots and continuous tracking of computer program activity. She also recommended that all data collected by the software be deleted.

READ: *Investigation Reports Summary*, page 12.

DOWNLOAD: *Use of Employee Monitoring Software by the District of Saanich* (oipc.bc.ca).

Personal Information Protection Act (PIPA) Reviewed

A robust law, revisited: a comprehensive review of the private sector privacy law by a Special Committee of the Legislature was undertaken in 2014.

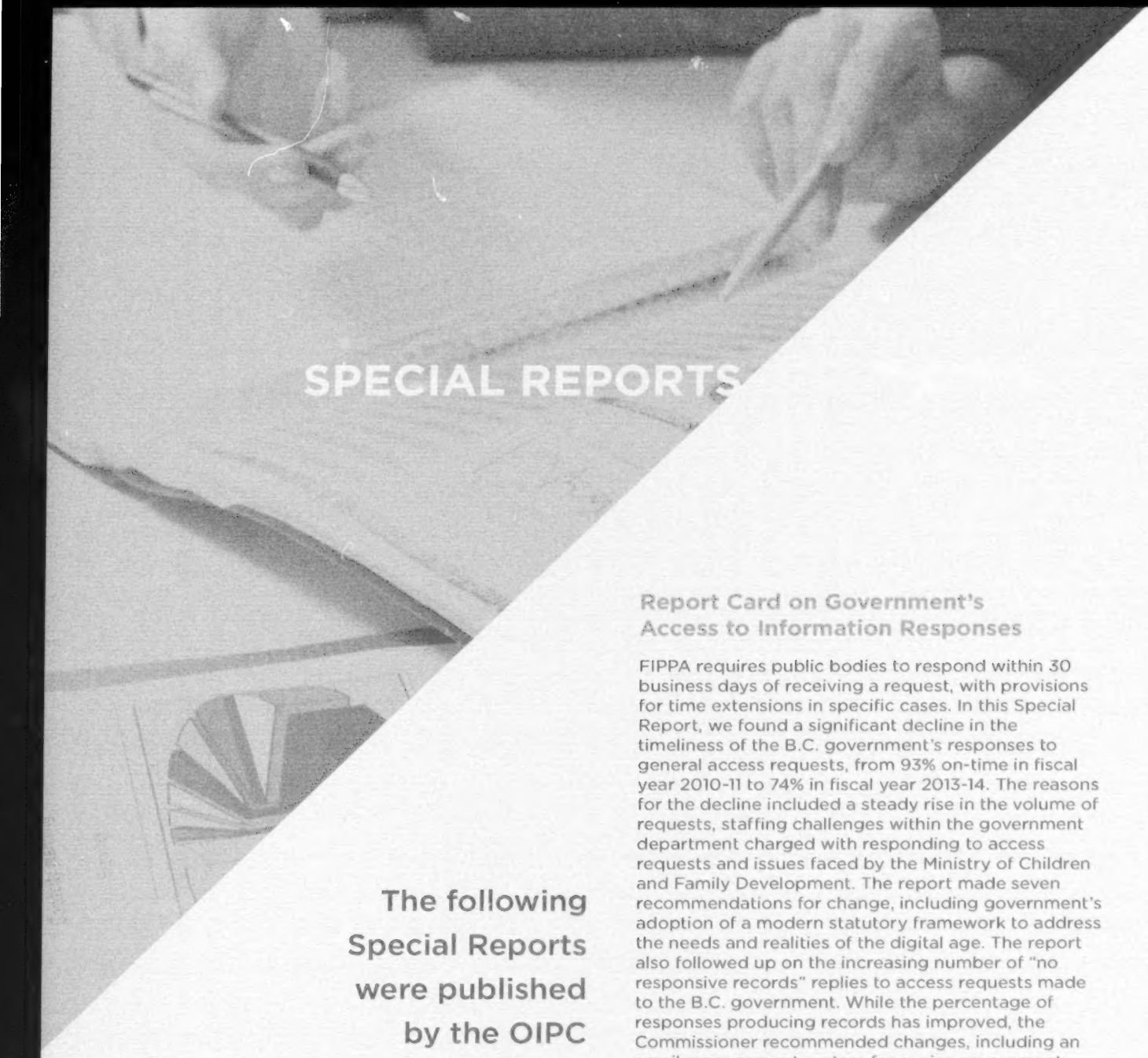
READ: *Mandate for Change*, page 20.

Report Card on B.C. Government's Access to Information Responses

This Special Report addresses the significant decrease in the timeliness of the B.C. Government's responses to access to information requests. Additional attention is needed to improve government's performance.

READ: *Special Reports Summary*, page 10.

DOWNLOAD: *A Step Backwards: Report Card on Government's Access to Information Response* (oipc.bc.ca).



SPECIAL REPORTS

The following Special Reports were published by the OIPC in 2014-15

Report Card on Government's Access to Information Responses

FIPPA requires public bodies to respond within 30 business days of receiving a request, with provisions for time extensions in specific cases. In this Special Report, we found a significant decline in the timeliness of the B.C. government's responses to general access requests, from 93% on-time in fiscal year 2010-11 to 74% in fiscal year 2013-14. The reasons for the decline included a steady rise in the volume of requests, staffing challenges within the government department charged with responding to access requests and issues faced by the Ministry of Children and Family Development. The report made seven recommendations for change, including government's adoption of a modern statutory framework to address the needs and realities of the digital age. The report also followed up on the increasing number of "no responsive records" replies to access requests made to the B.C. government. While the percentage of responses producing records has improved, the Commissioner recommended changes, including an email management system for senior government officials to ensure documents are preserved and archived. Finally, the report examined government's issuance of fee estimates in response to access requests, to determine whether they were being used to discourage applicants from pursuing a request. The report did not find evidence of this practice, but instead found government to be working with applicants to narrow broad requests to focus on records of particular interest.

DOWNLOAD: *A Step Backwards: Report Card on Government's Access to Information Responses* (oipc.bc.ca).

Improving Privacy Protection in the Health Sector

Concerned about how sensitive personal health information is protected in law and policy, the Commissioner examined the shortfalls of the current legislative framework in a Special Report about privacy protection in B.C.'s health sector. In it, she made 21 recommendations, urging the government to take a holistic approach to the collection, use, disclosure and protection of personal health information and patient data by introducing a comprehensive health information privacy law with independent oversight and enforcement. The Ministry announced it will consult with citizens about how to improve the current framework for managing health information and privacy concerns. We continue to stress that secure and controlled access to personal data is fundamental to building and maintaining trust in the health care system.

DOWNLOAD: *A Prescription for Legislative Reform* (oipc.bc.ca).

Modernizing Archives and Information Management

The Commissioner launched an examination into the state of British Columbia's archives after learning that tens of thousands of boxes containing valuable government records had been accumulating in warehouses for more than 10 years, rather than being deposited and preserved in the BC Archives. The archival institution, which was established in 1894, was merged with the Royal BC Museum in 2003. The Special Report made three recommendations to rectify the situation and modernize B.C.'s records management program. The Ministry of Technology, Innovation and Citizens' Services and the Museum have agreed to a stable funding model to assist in the reduction of the backlog. The agreement includes an upfront payment for the storage of government records being transferred to the BC Archives for the first 20 years as well as an annual commitment of up to $400,000 to cover the costs of preservation and making records available to the public.

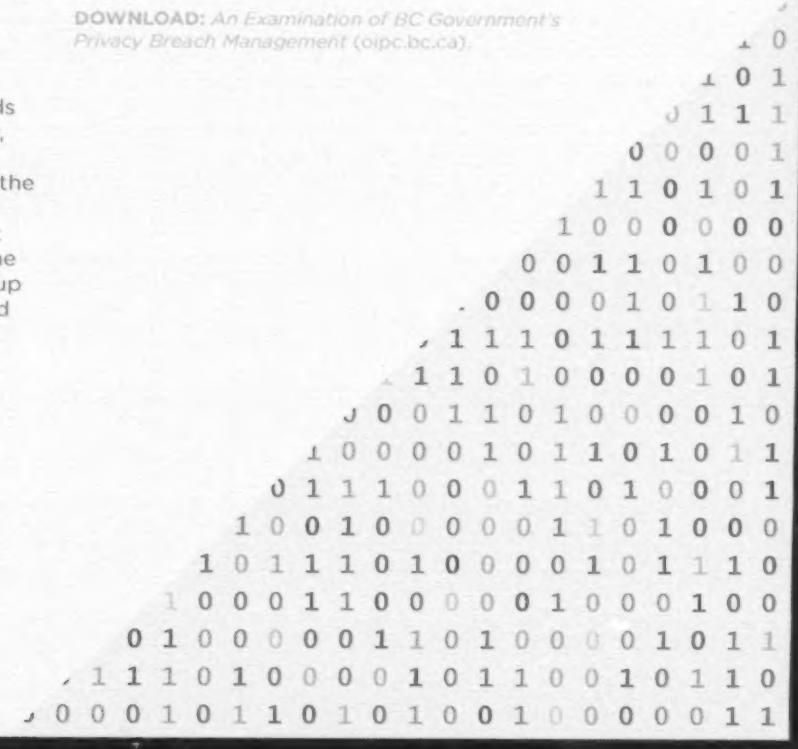
DOWNLOAD: *A Failure to Archive* (oipc.bc.ca).

Evaluating B.C. Government's Privacy Breach Management

The first report in the OIPC's new audit and compliance program examined the B.C. government's privacy breach management. The report reviewed the policies, procedures and training within government as well as more than 300 privacy breach reviews completed by government's central breach management agency. The Commissioner acknowledged the solid foundation government has in place for privacy breach management, but expressed concern about the lack of comprehensive and proactive breach analysis. The report offered five recommendations to help government enhance its breach management program, including the provision of ongoing training and awareness of the importance of protecting personal information and breach management processes. The OIPC will continue to examine breach management practices across the broader public sector in 2015, beginning with health authorities.

READ: *In Data We Trust*, page 22.

DOWNLOAD: *An Examination of BC Government's Privacy Breach Management* (oipc.bc.ca).



INVESTIGATION REPORTS

The following Investigation Reports were published by the OIPC in 2014-15

Police Information Checks

This comprehensive investigation of the misuse of police information checks in employment screening is the Commissioner's most important report to date. In response to the report, the Ministry of Justice announced a new province-wide policy that puts an end to the disclosure of mental health information in all police information checks, and halts the disclosure of non-conviction information by police for positions outside of the vulnerable sector. The policy has been adopted by all municipal police departments and the B.C. RCMP.

READ: *Protecting Privacy in Hiring*, page 18.

DOWNLOAD: *Use of Police Information Checks in British Columbia* (oipc.bc.ca).

District of Saanich Employee Monitoring Software

When the District of Saanich's use of employee monitoring software became a matter of public concern, the Commissioner initiated a proactive investigation to assess whether the use of monitoring software by the District complied with FIPPA. The software tools used by the District included keystroke logging, automated screen shots and continuous tracking of computer program activity. The investigation found that these tools violate the privacy rights of employees and recommended that the District disable them and destroy all data collected by the software. The District has agreed to implement all five of the report's recommendations, including the implementation of a comprehensive privacy management program and the appointment of a privacy officer for the District of Saanich.

DOWNLOAD: *Use of Employee Monitoring Software by the District of Saanich* (oipc.bc.ca).

Summary of Compliance with OIPC Special and Investigation Reports 2014-15

INVESTIGATION/ SPECIAL REPORT	TITLE	STATUS
April 15, 2014	*Use of Police Information Checks in British Columbia*	The Ministry of Justice developed a policy that prohibits disclosure of mental health information and prohibits the disclosure of non-conviction information for positions outside of those working with children or vulnerable adults. We continue to monitor implementation of the policy by police agencies and remain committed to encouraging government to develop a legislative framework for record checks.
April 30, 2014	*A Prescription for Legislative Reform: Improving Privacy Protection in B.C.'s Health Sector*	The Ministry of Health is studying the OIPC's recommendations, which include a call for a new health information law and increased individual rights to health records. The Ministry is currently consulting with stakeholders about new health information legislation in 2015.
July 22, 2014	*A Failure to Archive: Recommendations to Modernize Government Information Management*	Government has introduced and passed the *Information Management Act*. The Ministry of Technology, Innovation and Citizens' Services has come to an agreement with the Royal BC Museum to provide an upfront payment for the storage of government records being transferred to the BC Archives for the first 20 years as well as to provide annual funding of up to $400,000 to address the archiving backlog. The Ministry and the Museum have agreed to create a single integrated digital archive.
September 23, 2014	*A Step Backwards: Report Card on Government's Access to Information Responses April 1, 2013-March 31, 2014*	Government has taken positive steps on many recommendations but has not yet implemented a means of ensuring documentation of key government decisions. The OIPC will revisit their progress in 2015 to report on government's timeliness, backlog of requests and proactive disclosure.
January 28, 2015	*An Examination of BC Government's Privacy Breach Management*	Government has taken steps toward implementation of each of the Commissioner's five recommendations and is providing more information on breaches to this office, as well as updates on steps they are taking to address systemic issues. Staff in the Office of the Chief Information Officer are also working with ministries to target areas where deficits exist in training participation rates. The OIPC will continue to work with government throughout 2015 toward full implementation of the recommendations.
March 30, 2015	*Use of Employee Monitoring software by the District of Saanich*	The District of Saanich has disabled the Spector 360 software and agreed to comply with the OIPC's five recommendations, including appointing a Privacy Officer and implementing a comprehensive privacy management program.

PRIVACY WATCH

When the federal government introduced legislation in 2014 that could expand the powers of law enforcement, national security and intelligence agencies, Commissioner Denham and other Canadian Privacy and Information Commissioners responded quickly, calling for transparency and a public debate on the privacy impacts of the proposed bills.

It was a solemn statement of solidarity. Canada's federal, provincial and territorial Privacy and Information Commissioners gathered in Ottawa for their annual meeting on October 28-29, just days after the fatal attacks on Parliament Hill and in Saint-Jean-sur-Richelieu, Quebec. In a joint statement, the Commissioners expressed their condolences to the grieving families and friends of the fallen servicemen. They also made a strong and principled statement about the legislative changes publicly contemplated by the federal government in the wake of these troubling events — changes that would broaden the powers of intelligence and law enforcement agencies in Canada.

"We acknowledge that security is essential to maintaining our democratic rights. At the same time, the response to such events must be measured and proportionate, and crafted so as to preserve our democratic values," they wrote. The Commissioners called for an evidence-based approach to any additional powers for intelligence and law enforcement. They also recommended an open and transparent dialogue with Canadians about whether these new police powers were needed, and their impact on citizens' rights and freedoms should they be implemented.

The federal government has introduced several pieces of legislation that expand the powers of law enforcement, national security and intelligence agencies. The most notable among them is Bill C-51, the Anti-Terrorism Act.

Citizens, civil society groups, legal experts and Privacy Commissioners have all raised serious concerns about the provisions of Bill C-51. A joint letter from provincial and territorial Privacy Commissioners to the Parliamentary Committee studying the Bill expressed deep concern about the implications to the fundamental privacy rights of Canadians.

"Bill C-51 challenges fundamental rights and freedoms on several fronts, but the focus of our concern is on its mandate for overbroad, unregulated and intrusive sharing of the personal information of ordinary Canadians," they said. "If enacted [the Bill] would significantly expand the power of the state to surveil and profile ordinary, law-abiding Canadians."

DOWNLOAD: *Statement from B.C. Privacy Commissioner regarding Bill C-13; Statement of the Privacy and Information Commissioners of Canada on National Security and Law Enforcement Measures; Letter to the Standing Committee on Public Safety and Security re: Bill C-51 – the Anti-Terrorism Act* (oipc.bc.ca).

Concern about the erosion of privacy rights also motivated Commissioner Denham to speak out about the provisions of another piece of federal legislation, Bill C-13 (Protecting Canadians from Online Crime Act). "I am deeply concerned about the privacy implications of Bill C-13 and the proposed changes to law enforcement powers," she wrote in May 2014. "Similar provisions were introduced by the federal government in Bill C-30, the so-called lawful access legislation. Bill C-30 was vigorously opposed by many Canadians and civil society groups, and was also a cause of great concern to Privacy Commissioners across Canada. I have the same fundamental concerns about the law enforcement provisions of Bill C-13 as I had with Bill C-30." In June 2014 Commissioner Denham joined with her counterparts in Alberta and Ontario, calling for the Parliamentary Committee reviewing Bill C-13 to hear testimony from the Privacy Commissioner of Canada or other provincial and territorial Privacy Commissioners before making any decisions about the Bill.

While acknowledging that the world is changing, and that law enforcement agencies need the tools to be able to do their work effectively, Commissioner Denham maintains that the proponents of these new powers for intelligence and law enforcement agencies have failed to make the case that such broad and intrusive measures are necessary. New powers are being introduced without the necessary meaningful oversight of the activities of national security agencies.

There are legitimate circumstances in which surveillance and intelligence gathering is necessary for national security but these new powers cannot come at the expense of our constitutionally protected privacy rights, explains Denham. "The antidote is transparency," she says. "Shine a light on those programs. Let's have a debate about what we as a society are willing to accept — and what we are not prepared to accept — when it comes to national security and surveillance programs."

That debate, she stresses, is not about maintaining the state's surveillance capabilities. "It's about trying to determine the proper balance in the evolving information age." ■

GLOBAL GUARDIANS

An active participant in national and international privacy conversations, the OIPC works closely and collaboratively with colleagues at home — and around the world.

Data needs no passport. It flows freely over international borders and speaks all languages. Left unprotected, it has the potential to cause harm to individuals and disrupt global trade. International collaboration plays a critical role in ensuring the protection of personal information in our digital age, says Commissioner Denham. "When we collaborate with other privacy guardians, we improve the efficiency and effectiveness of our office, so that we may better serve the public here in B.C."

In addition to its work with Canadian privacy offices and organizations, the OIPC is an active member of two international privacy associations. The Office joined the Global Privacy Enforcement Network (GPEN) in 2012. Founded in 2010 to facilitate cross-border cooperation in the enforcement of privacy laws, GPEN achieves its goals through advocacy, enforcement and communications efforts. Monthly teleconference calls feature prominent guest speakers, while annual Privacy Sweeps provide a global snapshot of emerging privacy issues.

In 2014, 26 privacy regulators in 19 countries participated in the GPEN Internet Sweep, which took place May 12-18. Participants scrutinized 1,211 popular mobile apps and found that an overwhelming majority of those that collect personal information fail to provide an upfront privacy policy to users. Privacy authorities brought these results directly to app marketplaces in a joint letter following the sweep, including Microsoft, Google Play and the Apple App Store. "As the demand for mobile technologies continues to grow, it is important for app developers to let users know what personal information is being collected and why," Denham says.

DOWNLOAD: *Letter from Privacy Commissioners of Canada, United Kingdom, Australia and Macau regarding Insecam webcam website; Joint Open Letter to App Marketplaces* (oipc.bc.ca).

The OIPC has also been a member of the Asia Pacific Privacy Authorities (APPA) forum since 2010. Founded in 1992 for privacy regulators in the Asia Pacific region, APPA's members convene twice each year to form partnerships and exchange ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints. Issues explored by past forums have included privacy and security, a World Anti-Doping Code, cross-jurisdictional law enforcement in the Pacific Rim, privacy law reform, cryptography and big data.

From December 1-4, 2014, the OIPC was honoured to co-host the 42nd APPA Forum in Vancouver, together with the Privacy Commissioner of Canada. The meeting was attended by a broad range of more than 130 APPA delegates, guests, presenters and invited observers. In addition to information sharing and reporting by the delegates, the event also offered sessions and presentations from academics, industry and civil society groups on topics such as wearable technologies, the Right to be Forgotten, cross border trade and privacy regulation and accountability.

The experiences gleaned from these information networks can provide an early warning system for member regulators, as privacy issues often emerge in one jurisdiction before the others. Information sharing also takes place through secondments, which are temporary work assignments and exchanges between participating offices. In February 2015, an OIPC investigator was seconded to the Office of the Privacy Commissioner for Hong Kong for six weeks, charged with writing a report on his observations of their operations.

By engaging in the global conversation about privacy and access, whether it's about the privacy of mobile apps, the beta testing of Google Glasses or the Russian website Insecam's unwarranted aggregation and disclosure of live video footage, the OIPC is better able to serve the people of British Columbia. Data may flow unchecked across borders — but so too does knowledge.

PROTECTING PRIVACY IN HIRING

The Commissioner's investigation of the misuse of police information checks as an employment screening tool highlighted the profound impact the release of this sensitive personal information has had on British Columbians. Her recommendations ensure the correct balance between an individual's right to privacy and the legitimate business interests of employers.

Each year in B.C., thousands of police information checks are requested from police agencies and used by employers or volunteer groups in the hiring process. The information revealed can have a significant and lasting impact on an individual's privacy, human rights and feelings of dignity and self-worth.

Imagine that you've been asked to supply a police information check as a final step in a job process. Now picture what could happen behind the scenes if that check included information about your mental health, an attempted suicide, a complaint to police, an investigation that did not lead to a charge or other police contact that has not been proven in a court of law.

Shannon[1] was arrested for theft, a charge she vigorously denied. To her relief, Crown Counsel did not approve criminal charges. Later when she applied for a job, her prospective employer asked for a police information check. To her dismay, the check included the unfounded allegation. Though she explained the situation to the employer, he chose not to hire her due to this prior police concern.

Kim[2] was applying for her first professional job and had to supply a police information check. She had no criminal convictions and the police had never charged her with anything. Nonetheless, when Kim received the results of her check, it came back with an indication of a problem. The incident in question arose out of an argument at a party where police had been called. Kim alleged an individual had assaulted her and he, in turn, alleged that she had assaulted him. Kim never spoke to the police again about the incident and had no idea it would be caught by an employment-related record check. It was left to Kim to explain this incident to her prospective employer as she attempted to begin her career.

During the investigation, the Office received dozens of personal accounts from prospective employees and volunteers who had first-hand experience with police information checks in the hiring process. We also received detailed written submissions from employers and civil society groups about the impact of police information checks on individuals.

The Commissioner has described the investigation report, *Use of Police Checks in British Columbia*, as the most important she has issued to date. The report recommended that police forces immediately stop disclosing non-conviction information as part of employment-related record checks outside the vulnerable sector. She also recommended that mental health information never be included in any employment-related record check, regardless of the position. "Mental health information shou'd never be included in an employment-related record check. There is no reason why this information should be disclosed to employers, who would have no right to otherwise ask about this information in the hiring process," says the Commissioner. "Releasing this information threatens to further stigmatize the one in five of us who are affected by a mental health issue."

In response to the Commissioner's report and recommendations, B.C.'s Minister of Justice issued a policy directive to all police agencies in B.C. prohibiting the release of mental health information for any employee background checks. Specific non-conviction information can only be released in the context of checks for employees working with children and vulnerable adults. All municipal police agencies and the E division of the RCMP have implemented this directive — an important interim step prior to legislation, the Commissioner says. "There is no evidence that non-conviction information predicts a risk of future criminal behaviour, improves the safety of citizens, or results in better hiring decisions. With the exception of those working with children and vulnerable adults, non-conviction information should be considered off-limits in an employment-related record check." ■

DOWNLOAD: *Use of Police Information Checks in British Columbia* (oipc.bc.ca).

[1] Not her real name.
[2] Not her real name.

MANDATE FOR CHANGE

A thoughtful review of B.C.'s privacy law seeks to ensure that PIPA remains relevant and robust in our digital society.

Photo courtesy of the Legislative Assembly of British Columbia

When the *Personal Information Protection Act* ("PIPA") was first enacted in 2004, it was recognized as a leading piece of privacy legislation. The principles enshrined in PIPA, based on those established by the Organization for Economic Co-Operation and Development in 1980, are fundamentally sound and just as relevant today. "Our comprehensive private sector privacy law applies to more than 380,000 private organizations in B.C., including businesses, not-for-profits, charities, associations and trusts," says Commissioner Elizabeth Denham. "Every British Columbian consumer and employee has a right to privacy that is guaranteed and protected by PIPA."

But legislation is like a living organism — it must adapt to its environment. And what a rapidly changing environment it is, when you consider that 10 years ago, Twitter was unknown, Facebook still resided in a college dorm room and the word "big" was never used to describe data. All of these developments and many others have dramatically changed how organizations manage and use personal information.

A comprehensive review of the Act by an all-party Special Committee of the Legislative Assembly is mandated at least once every six years. The OIPC's involvement in the 2014 review began on May 28 with a general briefing to the Special Committee and a discussion of the current challenges to its effectiveness, including rapid technological change and a growing number of data security risks.

DOWNLOAD: *The Report of the Special Committee to Review the Personal Information Protection Act* (http://www.leg.bc.ca/cmt/40thparl/session-3/pipa/index.htm)
The OIPC Submission to the Special Committee to Review the Personal Information Protection Act (oipc.bc.ca).

The OIPC provided a written submission with 11 major recommendations for reform, including mandatory reporting of significant privacy breaches to affected individuals and the Commissioner's office. This type of breach notification regime would ensure B.C.'s PIPA is in harmony with the rules in Alberta as well as recent amendments to private sector privacy legislation at the federal level.

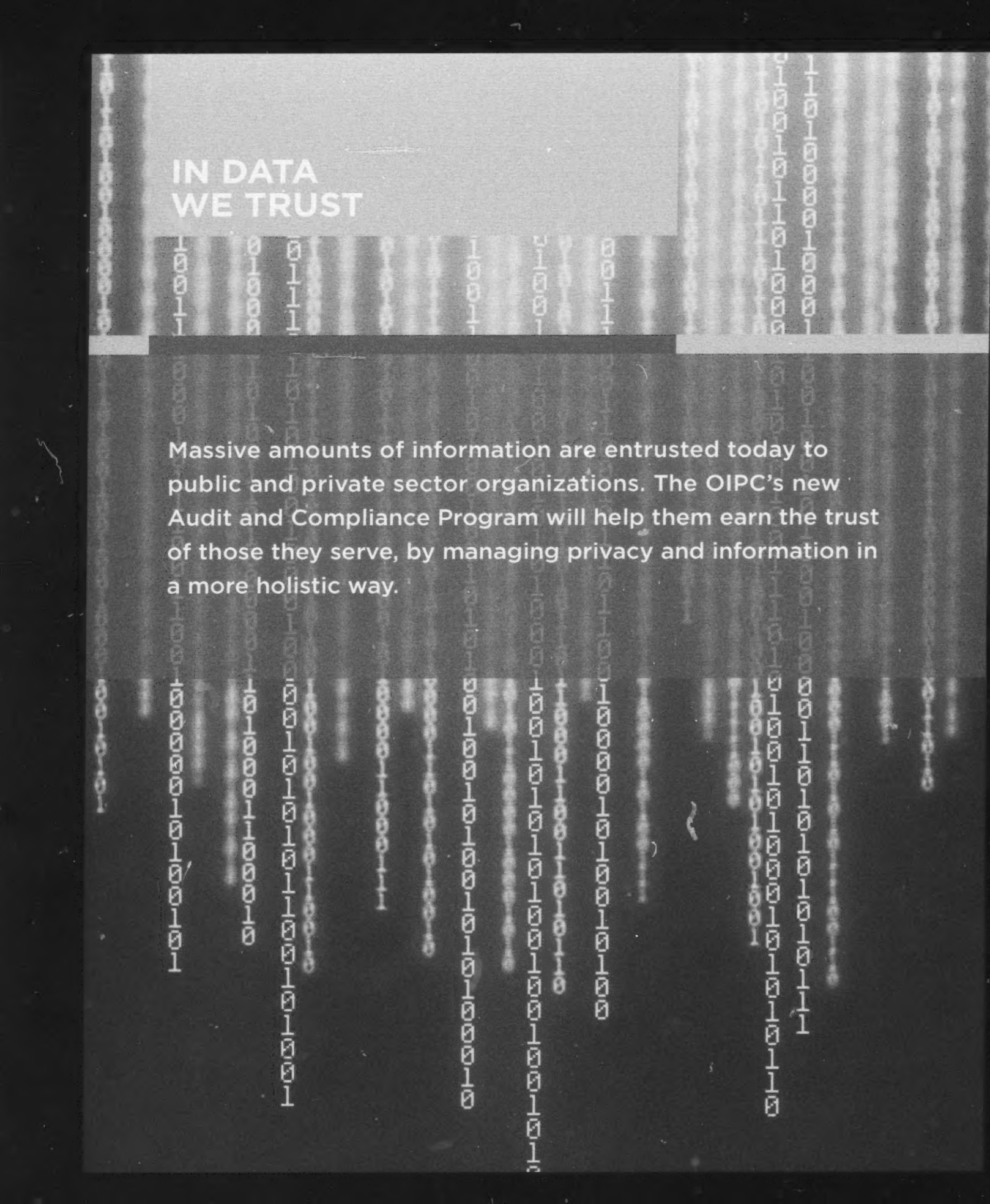
The OIPC's submission also recommended that PIPA be amended to include a requirement that organizations adopt privacy management programs that, among other things, make the privacy policies of the organization publicly available, include employee training and are regularly monitored and updated. While PIPA currently requires organizations to develop and follow privacy practices, these amendments would provide clarity as to the steps organizations must take to be more accountable for personal information they process.

In addition, the OIPC proposed a narrowing of PIPA's disclosure provisions, in light of a landmark decision of the Supreme Court of Canada. In *R v. Spencer*, the Court made it clear that law enforcement agencies require warrants to obtain information that would identify internet service subscribers. However, under B.C.'s PIPA, an organization may disclose personal information to a law enforcement agency without a warrant under section 18(1)(j). The OIPC recommended that the Committee bring the law into line with *Spencer*. The Commissioner also recommended transparency reporting, so that in future when organizations disclose personal information to law enforcement agencies without consent, there is a public accounting of that activity.

For nearly a year, the Special Committee studied the legislation, received public submissions and feedback and deliberated. With the publication of their final report, the Committee made 15 recommendations to strengthen consumer privacy rights and, importantly, bring B.C.'s laws into line with legislative reform underway in other jurisdictions. ■

IN DATA WE TRUST

Massive amounts of information are entrusted today to public and private sector organizations. The OIPC's new Audit and Compliance Program will help them earn the trust of those they serve, by managing privacy and information in a more holistic way.



What would it mean if the businesses and public agencies you deal with became truly accountable for their information and privacy practices — to you, their employees, their partners and the general public? With the launch of its new Audit and Compliance Program, the OIPC is telling organizations subject to B.C.'s public and private sector privacy legislation they need to do just that.

The new program assesses the extent to which public bodies and private organizations are protecting personal information, complying with access provisions and implementing accountability into their organization's DNA. "It was a logical next step for us to add a proactive compliance function to our Office," says Commissioner Denham. "We are interested in taking an in-depth look at not only individual breaches and complaints, but also the policies, programs, systems and controls needed to manage privacy and information across an organization in a comprehensive way." The OIPC has published an audit charter that lays out a step-by-step process for how the Office will select organizations to review, what information will be requested and the outcomes.

In the first report under the new program, *An Examination of B.C. Government's Privacy Breach Management*, issued in January 2015, the Office studied the degree to which the provincial government is fulfilling its duty to respond to and properly manage privacy breaches. Members of the public often have no choice but to hand over their personal information in exchange for government services such as health care, education, or other social benefits. They're understandably concerned about the protection of their privacy and need assurances that they can trust public bodies to safeguard their personal information.

The assessment revealed that government has a solid foundation in place for managing privacy breaches. The majority of suspected breaches are reported to the Office of the Chief Information Officer within a day or two of the incident and are contained and investigated within a reasonable timeframe. Ministries provided notifications to affected individuals when appropriate, and written notifications included all of the necessary information. The OCIO also provided advice on preventative measures in almost every investigation.

There were however opportunities for improvement; gaps were found in relation to audits of security safeguards, analysis and public reporting of breaches, follow-up on implementation of preventative measures, timeliness of notifying individuals who may have been impacted by a breach, internal processes for documenting and tracking breaches and training participation rates. There was also a lack of clarity about when breaches should be reported to the Information and Privacy Commissioner. In addition, the Office was notified of fewer than one percent of the actual privacy breaches. "When organizations and public bodies are proactive and report breaches to us, it gives my Office an opportunity to assist them in addressing the root causes of breaches and engage in learning and future prevention," says the Commissioner.

The report made five recommendations which, as they are implemented, will help government enhance the efficacy of its breach management program and build trust among citizens. The OIPC will continue to examine breach management practices across the broader public sector in 2015.

Vast amounts of personal information are held today by organizations and government agencies. Given the increasing number of privacy breaches, it's critical that agencies develop and strengthen their privacy management programs. The OIPC's Audit and Compliance Program was designed to ensure that happens. ■

DOWNLOAD: *An Examination of B.C. Government's Privacy Breach Management.* Learn more about the OIPC's Audit and Compliance Program (oipc.bc.ca).

YEAR IN NUMBERS

In 2014-15, citizens and consumers continued to think more about their privacy in all contexts and public bodies and organizations engaged our office more frequently.

Detailed information about the Year in Numbers can be found over the next eight pages. A summary of some of the key findings follows:

Files Opened

The OIPC opened 8,419 files in 2014-15. In 2013-14, 7,298 files were opened.

+15%

Requests for Information

In 2014-15, we received 5,200 requests for information. In 2013-14, we received 4,024.

+29%

Privacy Breaches

132 privacy breaches were reported to the Office in 2014-15. Last year: 114

+16%

Privacy Impact Assessments

33 PIAs were reviewed in 2014-15. In 2013-14: 20

+65%

Policy or Issue Consultation

The Office conducted 170 policy/issue consultations in 2014-15. Last year: 81

+110%

Media Inquiries

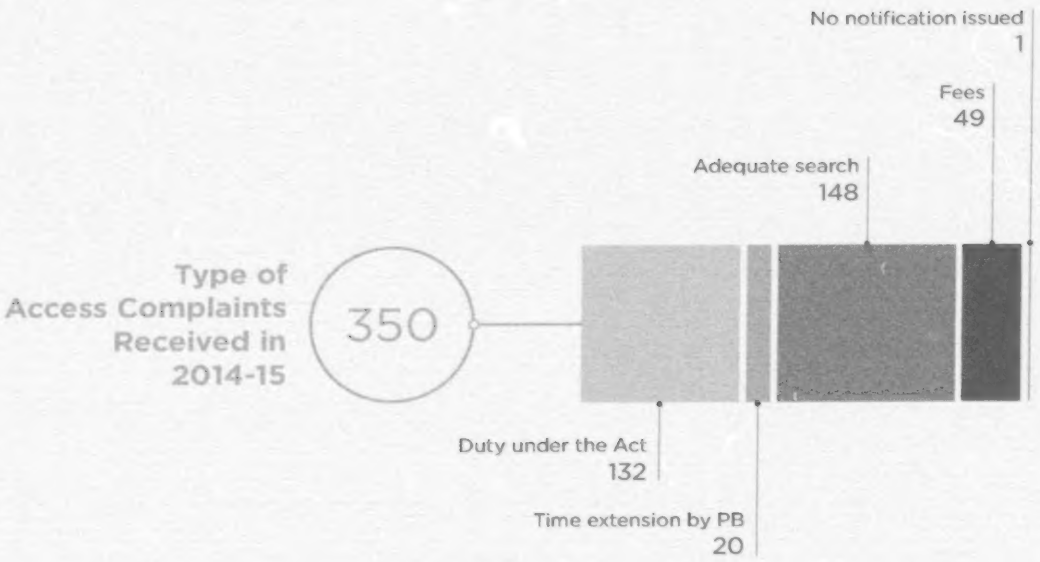
The Office received 262 media requests in 2014-15. In 2013-14: 180

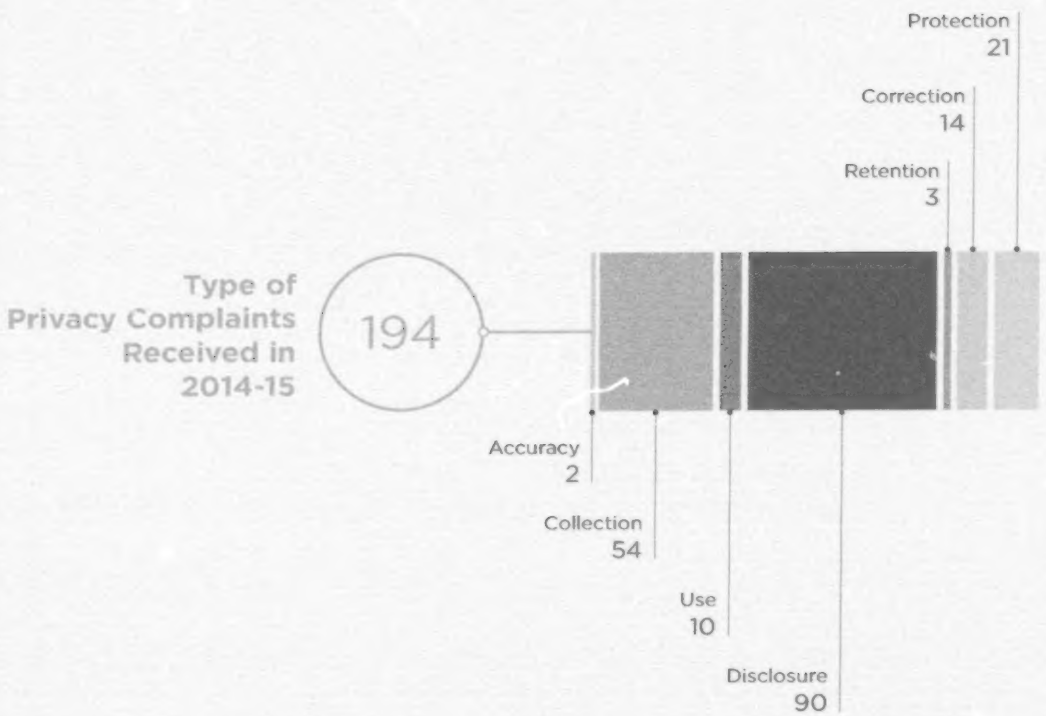
+46%

Summary of all FIPPA and PIPA files received in 2014-15

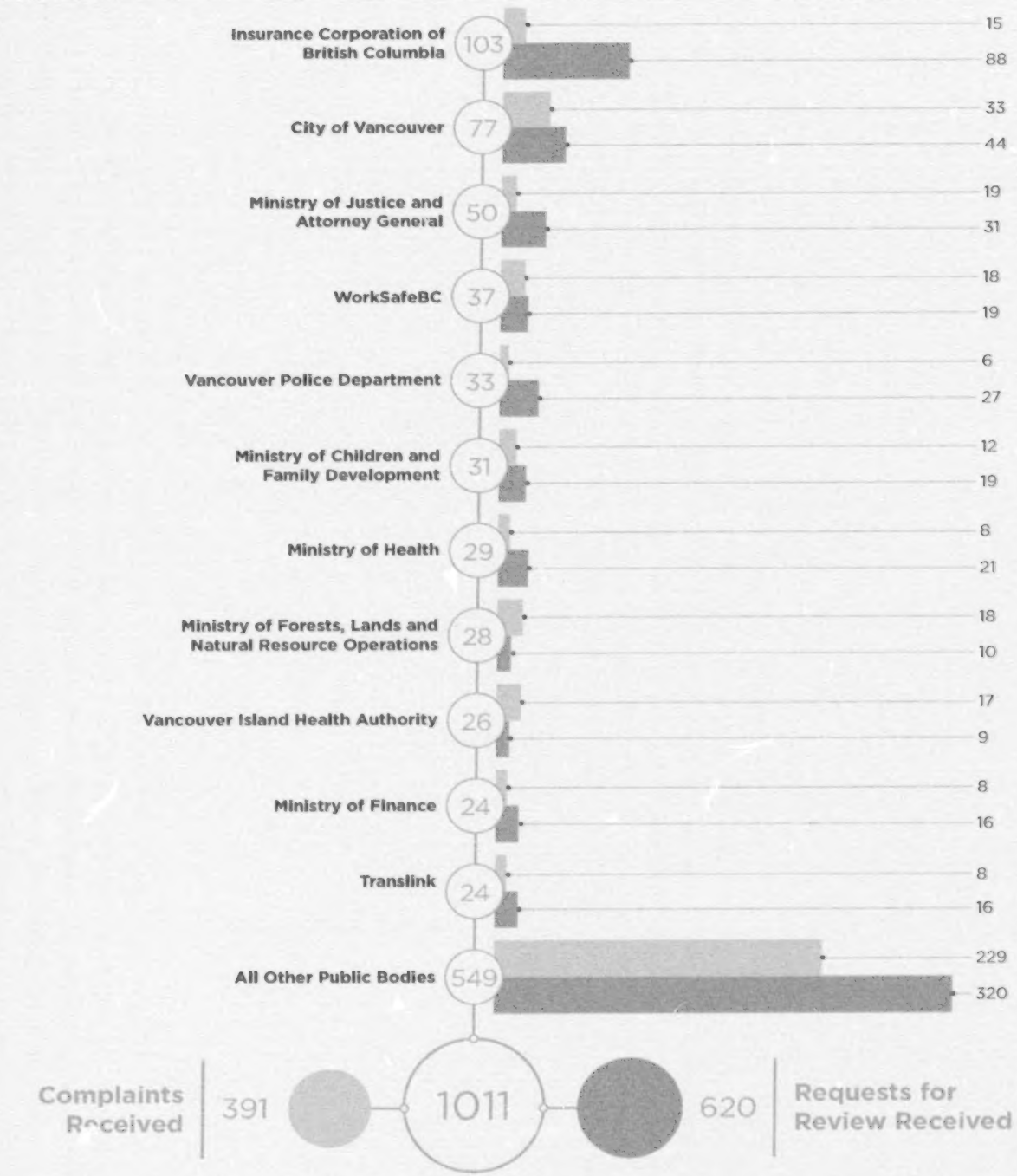
FILE TYPE	Received 2014-15	Received 2013-14	Received 2012-13
Complaints			
Access complaints	350	408	266
Privacy complaints	194	231	173
Requests for review			
Requests for review of decisions to withhold information	676	778	618
Applications to disregard requests as frivolous or vexatious	4	7	8
Time extensions			
Requests by public bodies and private organizations	721	853	735
Requests by applicants seeking a review	20	19	17
Reconsideration of decisions			
Internal reconsideration of OIPC decisions	23	27	16
Adjudication (court review of OIPC decisions)	2	2	1
Information requested			
Requests for information and correspondence received	5,200	4,024	4,346
Media inquiries	262	180	209
FOI requests for OIPC records	18	27	31
Non-jurisdictional issue	29	4	19
No reviewable issue	222	165	132
Files initiated by public bodies and private organizations			
Privacy impact assessments	33	20	21
Privacy breach notification	132	114	106
Public interest notification	14	17	17
Policy or issue consultation	170	81	137
Police Act IIO reports	19	37	5
Request for Contact Information (research)	1	2	2
OIPC initiatives			
Investigations	8	11	7
Legislative reviews	53	38	56
Projects	87	78	160
Public education and outreach			
Speaking engagements and conferences	67	96	99
Meetings with public bodies and private organizations	107	69	59
Site visits	0	4	1
Other	7	6	6
TOTAL	8,419	7,298	7,247

YEAR IN NUMBERS





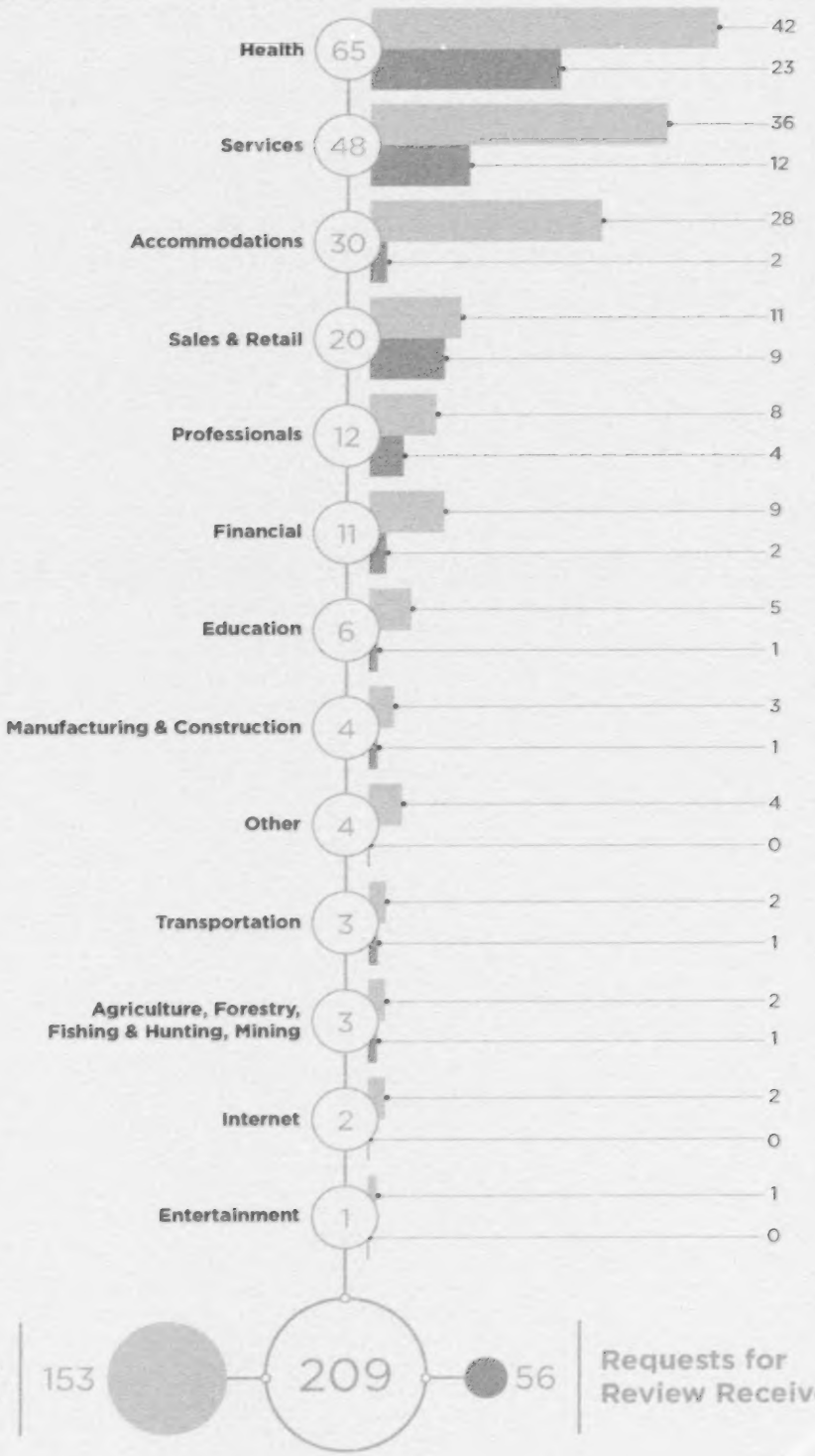
Number of FIPPA Complaints and Requests for Review Received in 2014-15 by Public Body



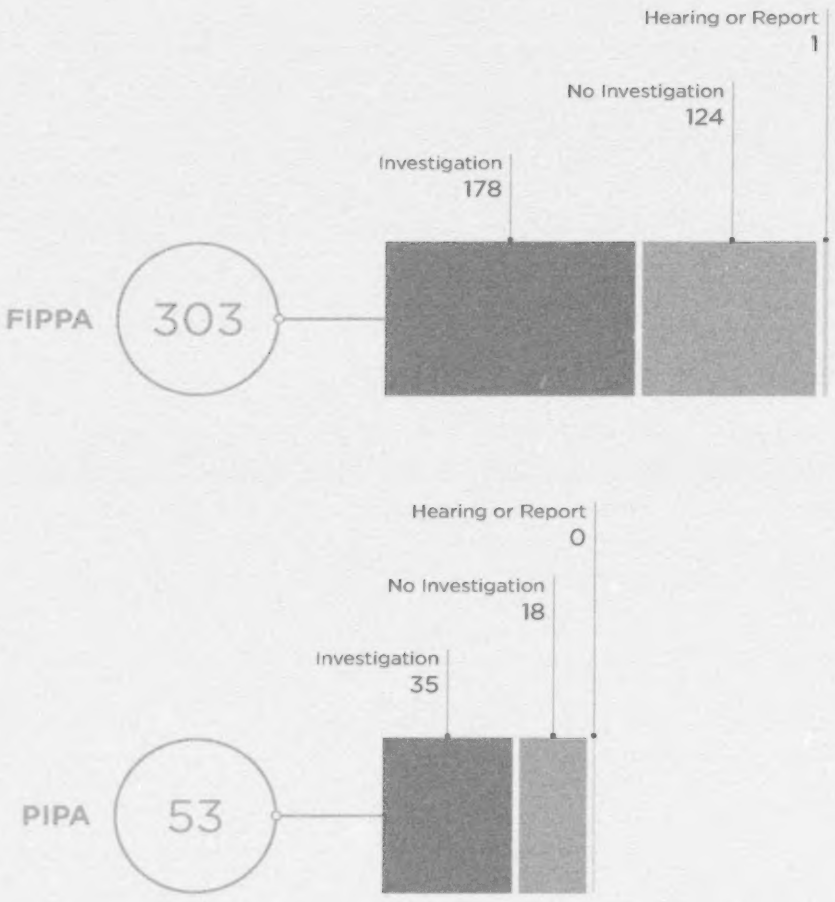
NOTE: The number of requests for review and complaints against a public body is not necessarily indicative of non-compliance, but it may be reflective of its business model or quantity of personal information involved in its activities. The majority of ICBC requests for review, for example, are filed by lawyers performing due diligence on behalf of clients involved in motor vehicle accident lawsuits.

YEAR IN NUMBERS

Number of PIPA Complaints and Requests for Review Received in 2014-15 by Sector



Outcome of Access Complaints Resolved in 2014-15



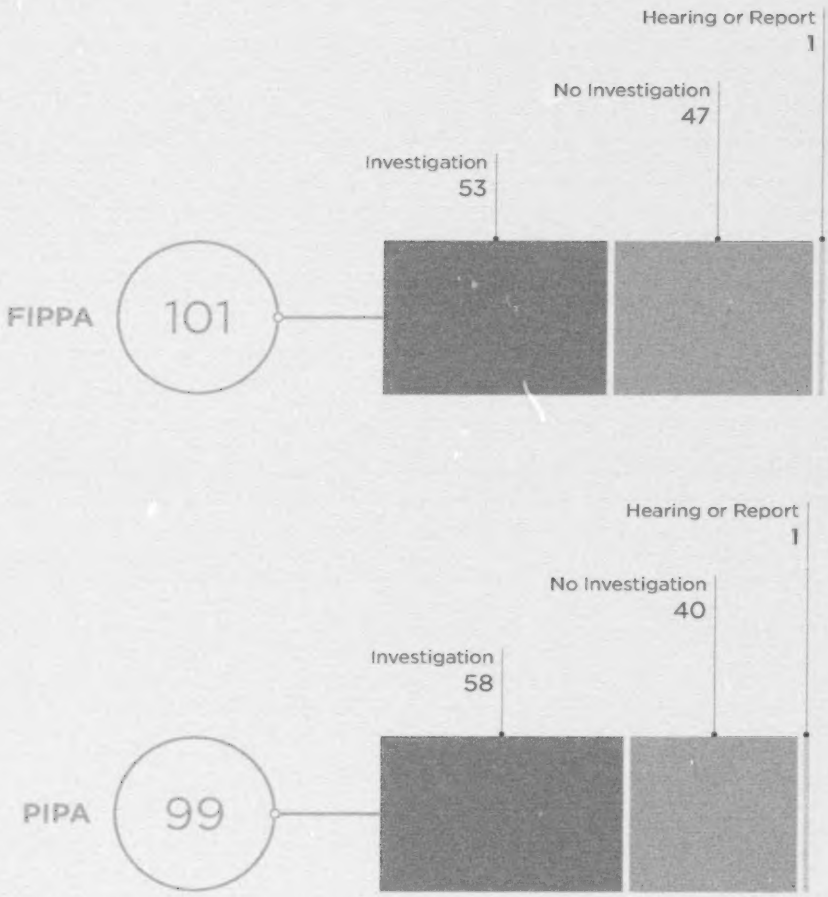
Investigation
Includes files that were mediated, not substantiated, partially substantiated and substantiated.

No Investigation
Includes files referred back to public body, withdrawn, or files the OIPC declined to investigate.

Hearing or Report
Refers to files that proceeded to inquiry and/or a report was issued.

YEAR IN NUMBERS

Outcome of Privacy Complaints Resolved in 2014-15

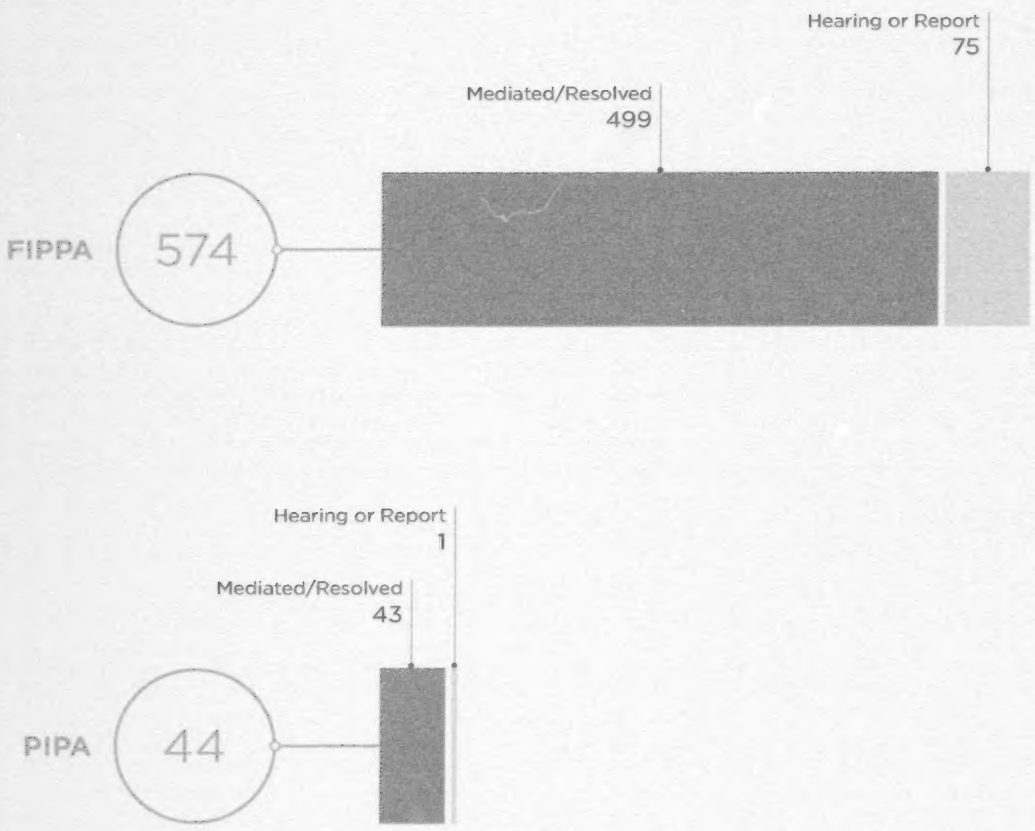


Investigation
Includes files that were mediated, not substantiated, partially substantiated and substantiated.

No Investigation
Includes files referred back to public body, withdrawn, or files the OIPC declined to investigate.

Hearing or Report
Refers to files that proceeded to inquiry and/or a report was issued.

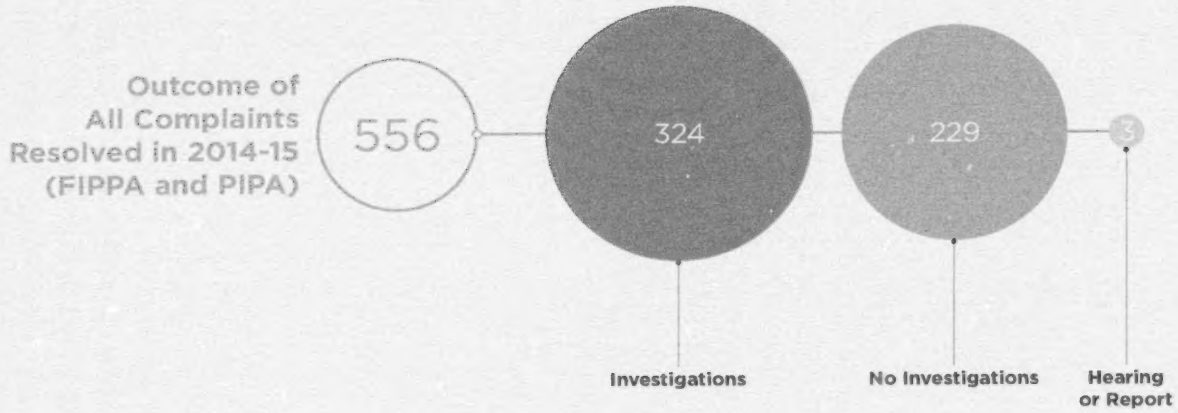
Outcome of Requests for Review Resolved in 2014-15



Mediated/Resolved
Includes files that were mediated, withdrawn, referred to public body, consent order or other decision by Commissioner.

Hearing or Report

YEAR IN NUMBERS



FINANCIAL REPORTING

Nature of Operations

The Information and Privacy Commissioner is an independent Officer of the Legislature, whose mandate is established under the *Freedom of Information and Protection of Privacy Act* ("FIPPA") and the *Personal Information Protection Act* ("PIPA"). FIPPA applies to more than 2,900 public agencies and accords access to information and protection of privacy rights to citizens. PIPA regulates the collection, use, access, disclosure and retention of personal information by more than 380,000 private sector organizations.

The Commissioner has a broad mandate to protect the rights given to the public under FIPPA and PIPA. This includes: conducting reviews of access to information requests, investigating complaints, monitoring general compliance with the Acts and promoting freedom of information and protection of privacy principles.

In addition, the Commissioner is the Registrar of the Lobbyists Registry program and oversees and enforces the provisions under the *Lobbyists Registration Act*.

Funding for the operation of the Office of the Information and Privacy Commissioner is provided through a vote appropriation (Vote 5) of the Legislative Assembly and through cost recovery from conferences hosted by the Office. The vote provides separately for operating expenses and capital acquisitions, and, all payments or recoveries are processed through the Province's Consolidated Revenue Fund. Any unused appropriation cannot be carried forward for use in subsequent years.

As well, part of the Office's funding is dedicated solely for the purpose of carrying out judicial review work, such as proceedings brought against the Office of the Information and Privacy Commissioner. Any portion of the dedicated funding that is unused for that purpose during the fiscal year is returned to the Consolidated Revenue Fund at fiscal year-end.

Accounting Policies and Procedures

This financial reporting has been prepared per the policies and procedures as set out in the Province of British Columbia's Core Policy and Procedures Manual (or CPPM), found at: http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm. Section 1.2.4, Governance, Application, describes the entities that are required to follow the CPPM which includes the Office of the Information and Privacy Commissioner.

Voted, Used and Unused Appropriations

The Office receives approval from the Legislative Assembly to spend funds through an appropriation that includes two components — operating and capital. Any unused appropriation cannot be carried forward for use in subsequent years.

The following table compares the Office's voted appropriations, total operating and capital expenses, and the total remaining unused appropriation (unaudited) for the current and previous fiscal year:

	2014-15		2013-14	
	Operating	Capital	Operating	Capital
Appropriation	$5,526,000	$45,000	$5,526,000	$45,000
Other amounts	$0	$0	$0	0
Total appropriation	$5,526,000	$45,000	$5,526,000	$45,000
Total operating expenses	$5,514,401	-	$5,321,734	-
Capital acquisitions	-	$16,991	-	$25,637
Unused appropriation	*$11,599	$28,009	$204,266	$19,363

**Note: The unused funding of $11,599 was returned to the Consolidated Revenue Fund at fiscal year-end.*

Leave Liability

Eligible employees are entitled to accumulate earned, unused vacation and other eligible leave entitlements as provided under their terms of employment or collective agreement. The liability for the leave is managed and held by the BC Public Service Agency. Accumulated leave liability for the Office of the Information and Privacy Commissioner for fiscal year 2014-15 is $54,217.

Tangible Capital Assets

Tangible capital assets are recorded at historical cost less accumulated depreciation. Depreciation begins when the asset is put into use and is recorded on the straight-line method over the estimated useful life of the asset.

The following table shows the Office's capital assets (unaudited):

			2014-15	2013-14
	Closing Cost	Closing Accumulated Amortization	Net Book Value (March 31, 2015)	Net Book Value (March 31, 2014)
Computer Hardware & Software	$238,212	($209,646)	$28,567	$33,337
Tenant Improvements	$552,302	($478,662)	$73,640	$184,101
Furniture & Equipment	$83,633	($59,462)	$24,170	$30,691
	$874,147	($747,770)	$126,377	$248,129

Leasehold Commitments

The Office of the Information and Privacy Commissioner has a leasehold commitment with 947 Fort Street Holdings Ltd. for building occupancy costs. Total payments for occupancy costs for the fiscal year 2014-15 were $549,112. Payments to 947 Fort Street Holdings Ltd. for office space for fiscal 2015-16 are estimated to be $593,830.

Pension and Retirement Benefits

The Office and all eligible employees contribute to the Public Service Pension Plan which is a multi-employer, defined benefit and joint trusteeship plan, established for certain British Columbia public service employees. The British Columbia Pension Corporation administers the plan, including payments of pension benefits to eligible employees. A board of trustees, representing plan members and employers, is responsible for overseeing the management of the plan, including investment of assets and administration of benefits.

The Plan is contributory and its basic benefits are based on years of service and average earnings at retirement. Under joint trusteeship, the risks and rewards associated with the Plan's unfunded liability or surplus are shared between the employers and the plan members and will be reflected in their future contributions.

The Office also pays for retirement benefits according to conditions of employment for employees excluded from union membership. Payments are made through the province's payroll system. The cost of these employee future benefits is recognized in the year the payment is made.

RESOURCES

Getting Started

- A guide to OIPC processes (FIPPA and PIPA)
- A guide to PIPA for business and organizations
- A guide to FIPPA for individuals
- Early notice and PIA procedures for public bodies

Access (General)

- How do I request records?
- How do I request a review?
- Instructions for written inquiries
- Time extension guidelines for public bodies
- Guidelines for conducting adequate search investigations (FIPPA)

Privacy (General)

- Guidelines to develop a privacy policy
- Privacy proofing your retail business
- Protecting personal information away from the office
- Identity theft resources
- Privacy guidelines for landlords and tenants
- Privacy emergency kit

Comprehensive Privacy Management

- Getting accountability right with a privacy management program
- Accountable privacy management in B.C.'s public sector

Privacy Breaches

- Key steps to responding to privacy breaches
- Breach notification assessment tool
- Privacy breach policy template
- Privacy breach checklist

Technology & Social Media

- Cloud computing guidelines (public and private sector)
- Good privacy practices for developing mobile apps
- Public sector surveillance guidelines
- Guidelines for overt video surveillance in the private sector
- Use of personal email accounts for public business
- Guidance for the use of body-worn cameras by law enforcement authorities
- Guidelines for online consent
- Guidelines for social media background checks

To request copies of these resources, or to get more information about B.C.'s access and privacy laws, email info@oipc.bc.ca or visit www.oipc.bc.ca

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Office of the Information and Privacy Commissioner for British Columbia

PO Box 9038, Stn. Prov. Govt., Victoria, BC V8W 9A4
Telephone: 250.387.5629 | Toll Free in B.C.: 1.800.663.7867
E-mail: info@oipc.bc.ca | @BCInfoPrivacy

www.oipc.bc.ca